



14-0024-TH(2)

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 1月26日

出 願 番 号
Application Number:

特願2000-016937

出 願 人
Applicant (s):

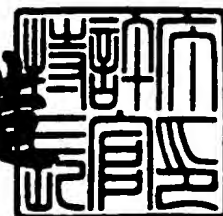
日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月 8日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 412000058

【提出日】 平成12年 1月26日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08
G09C 1/00

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 猪羽 渉

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 菅原 隆幸

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 日暮 誠司

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 黒岩 俊夫

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 上田 健二郎

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代表者】 守隨 武雄

【電話番号】 045-450-2423

【手数料の表示】

【予納台帳番号】 003654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法

【特許請求の範囲】

【請求項 1】

コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法において、

前記鍵情報を生成するにあたって、多数のビットからなる第 1 ビット列を有する前記鍵のもとになる情報を、前記第 1 ビット列よりビット数の少ない複数のビットからなる第 2 ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第 2 ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビット列よりビット数が少ないビット数の第 3 ビット列を出力する第 1 ステップと

前記第 1 ステップで出力した前記第 3 ビット列を入力するか、又は前記第 3 ビット列をこれよりビット数が少ないビット列に分割した第 4 ビット列を入力し、前記第 3 又は第 4 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 3 又は第 4 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 3 又は第 4 ビット列のビット数より少ないビット数の第 5 ビット列を前記鍵情報又は前記鍵情報の一部として出力する第 2 ステップとからなることを特徴とする鍵情報生成方法。

【請求項 2】

コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置において、

前記鍵情報を生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力するS-Boxと、

前記S-Boxから出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記鍵情報又は前記鍵情報の一部として出力する論理演算部とを備えたことを特徴とする鍵情報生成装置。

【請求項3】

第1鍵のもとになる情報を第2鍵で暗号化すると共に、前記第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、

前記第1鍵を生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則

に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビット列よりビット数が少ないビット数の第 3 ビット列を出力する第 1 ステップと

前記第 1 ステップで出力した前記第 3 ビット列を入力するか、又は前記第 3 ビット列をこれよりビット数が少ないビット列に分割した第 4 ビット列を入力し、前記第 3 又は第 4 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 3 又は第 4 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 3 又は第 4 ビット列のビット数より少ないビット数の第 5 ビット列を前記第 1 鍵又は前記第 1 鍵の一部として出力する第 2 ステップとからなることを特徴とするコンテンツ情報暗号化方法。

【請求項 4】

第 1 鍵のもとになる情報を第 2 鍵で暗号化すると共に、前記第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、

前記第 1 鍵を生成するにあたって、多数のビットからなる第 1 ビット列を有する前記鍵のもとになる情報を、前記第 1 ビット列よりビット数の少ない複数のビットからなる第 2 ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第 2 ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビット列よりビット数が少ないビット数の第 3 ビット列を出力する S - B o x と、

前記 S - B o x から出力した前記第 3 ビット列を入力するか、又は前記第 3 ビット列をこれよりビット数が少ないビット列に分割した第 4 ビット列を入力し、前記第 3 又は第 4 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 3 又は第 4 ビット列のビット数よ

り少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記第1鍵又は前記第1鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報暗号化装置。

【請求項5】

暗号化した第1鍵のもとになる情報を第2鍵で復号化すると共に、復号化後の第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、

前記第1鍵を生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力する第1ステップと

前記第1ステップで出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記第1鍵又は前記第1鍵の一部として出力する第2ステップとからなることを特徴とするコンテンツ情報復号化方法。

【請求項6】

暗号化した第1鍵のもとになる情報を第2鍵で復号化すると共に、復号化後の第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、

前記第1鍵を生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力するS-Boxと、

前記S-Boxから出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記第1鍵又は前記第1鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報復号化装置。

【請求項7】

請求項3記載のコンテンツ情報暗号化方法、もしくは、請求項4記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第1鍵のもとになる情報とを記録媒体に記録したことを特徴とするコンテンツ情報記録媒体。

【請求項8】

請求項3記載のコンテンツ情報暗号化方法、もしくは、請求項4記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第

1 鍵のもとになる情報とを伝送路を介して送信することを特徴とするコンテンツ情報伝送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツ情報を暗号化したり、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する、鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法に関するものである。

【0002】

【従来の技術】

近年、デジタル化が進み、デジタル化された映像信号や音声情報などのコンテンツ情報を記録媒体に記録して再生したり、あるいは、ソフトウェアやデータなどのコンテンツ情報をネットワークにより伝送することが盛んに行われている。

【0003】

そして、著作権を有し且つデジタル化されたコンテンツ情報（以下、デジタル情報と記す）の不正使用を防止する場合、デジタル情報に対して所定の暗号化鍵を用いて暗号化し、この暗号化したデジタル情報を磁気テープ、磁気ディスク、光ディスク、カード等の記録媒体に記録したり、あるいは、暗号化したデジタル情報をネットワークを介して伝送したりしている。この後、記録媒体やネットワークを介して提供された暗号化済みのデジタル情報は、暗号化鍵と等価の復号化鍵を用いて復号化されて暗号化前のデジタル情報に戻している。

【0004】

一方、DES (Data Encryption Standard) 暗号化方法は、アメリカ商務省標準局（現在、NIST: National Institute of Standard Technology）が決めた暗号標準であり、現在もつと多く用いられている暗号化方法の一つである。このDES暗号化方法では、64ビット平文入力が64ビット暗号文出力に変換

される。この際、暗号化鍵も平文入力と同じように 64 ビット構成であるが、そのうちの 8 ビットをパリティに使っているので、実質的な暗号化鍵は 56 ビット構成となっている。

【0005】

図4は一般的なDES (Data Encryption Standard) 暗号化方法に用いられているS-Boxを示したブロック図である。

【0006】

図4に示した如く、DES (NIST.FIPS Publication 46-1:Data Encryption Standard.January 22,1988) 暗号化方法に用いられているS-Box (Selection-Box) は、6ビットの入力に対して4ビットを出力する、一方向性関数の一種である。この種の一方向性関数Fは、一方向性ハッシュ関数 (One-Way Hash Function)、又は単に、ハッシュ関数と呼ばれる、 x から $F(x)$ を計算するのは容易であるが、 $F(x)$ から x を求めるのは極めて困難な関数 $F(x)$ を用いている。

【0007】

また、上記したS-Boxは二次元のテーブルTを持っていて、4行×16列のテーブルT内に行と列とに対応させて各要素値Hが0から15までの16進の整数で予め設定されている。そして、入力の6ビットを例えば " $b_5b_4b_3b_2b_1b_0$ " とすると、" b_5 " と " b_0 " の2ビットでテーブルTの行を指定し、また " b_5 " と " b_0 " の2ビットを除いた " $b_4b_3b_2b_1$ " の4ビットでテーブルTの列を指定し、ここで指定した行列の部位と対応して4ビットからなる一つの要素値Hを出力している。

【0008】

上記した具体例を図4に示すと、S-Boxへの入力6ビットを例えば " 100100 " とした時、" 10 " 行 " 0010 " 列、すなわち、2行2列の要素値9 ($=1001$) を出力している。

【0009】

【発明が解決しようとする課題】

ところで、公知のS-Boxを用いて鍵のもとになる情報から、暗号化及び復

号化に必要な暗号化鍵及び復号化鍵を生成するために必要な一方向性関数を求めようとする場合、上記した S-B o x では入力ビットの“0”と“1”との割合を直接反映しないでテーブル T から出力を得ることができるので、これを用いて暗号化鍵及び復号化鍵の生成に好適なシステムを実現することが可能である。

【0 0 1 0】

しかしながら、暗号化及び復号化に必要な暗号化鍵及び復号化鍵を生成する際に、上記した S-B o x により例えば 6 ビットの入力に対して 4 ビットを出力するのでは、一定のビット数を減らす一方向性関数しか構成できず、しかも、少ないステップ数で大きなビット数の入力に対して小さなビット数に減らし、かつ任意にその圧縮率を変えられるような一方向性関数を構成することはできないなど問題点が生じている。

【0 0 1 1】

【課題を解決するための手段】

本発明は上記課題に鑑みてなされたものであり、第 1 の発明は、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法において、

前記鍵情報を生成するにあたって、多数のビットからなる第 1 ビット列を有する前記鍵のもとになる情報を、前記第 1 ビット列よりビット数の少ない複数のビットからなる第 2 ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第 2 ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビット列よりビット数が少ないビット数の第 3 ビット列を出力する第 1 ステップと、前記第 1 ステップで出力した前記第 3 ビット列を入力するか、又は前記第 3 ビット列をこれよりビット数が少ないビット列に分割した第 4 ビット列を入力し、前記第 3 又は第 4 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 3 又は第 4 ビット列のビット数より

少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記鍵情報又は前記鍵情報の一部として出力する第2ステップとからなることを特徴とする鍵情報生成方法である。

【0012】

また、第2の発明は、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置において、前記鍵情報を生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力するS-Boxと、前記S-Boxから出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記鍵情報又は前記鍵情報の一部として出力する論理演算部とを備えたことを特徴とする鍵情報生成装置である。

【0013】

また、第3の発明は、第1鍵のもとになる情報を第2鍵で暗号化すると共に、前記第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第

1 鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、前記第 1 鍵を生成するにあたって、多数のビットからなる第 1 ビット列を有する前記鍵のもとになる情報を、前記第 1 ビット列よりビット数の少ない複数のビットからなる第 2 ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第 2 ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビット列よりビット数が少ないビット数の第 3 ビット列を出力する第 1 ステップと、前記第 1 ステップで出力した前記第 3 ビット列を入力するか、又は前記第 3 ビット列をこれよりビット数が少ないビット列に分割した第 4 ビット列を入力し、前記第 3 又は第 4 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 3 又は第 4 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 3 又は第 4 ビット列のビット数より少ないビット数の第 5 ビット列を前記第 1 鍵又は前記第 1 鍵の一部として出力する第 2 ステップとからなることを特徴とするコンテンツ情報暗号化方法である。

【 0 0 1 4 】

また、第 4 の発明は、第 1 鍵のもとになる情報を第 2 鍵で暗号化すると共に、前記第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、前記第 1 鍵を生成するにあたって、多数のビットからなる第 1 ビット列を有する前記鍵のもとになる情報を、前記第 1 ビット列よりビット数の少ない複数のビットからなる第 2 ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第 2 ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビッ

ト列よりビット数が少ないビット数の第3ビット列を出力するS-B o xと、前記S-B o xから出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記第1鍵又は前記第1鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報暗号化装置である。

【0015】

また、第5の発明は、暗号化した第1鍵のもとになる情報を第2鍵で復号化すると共に、復号化後の第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、

前記第1鍵を生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力する第1ステップと、前記第1ステップで出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果

のビットで前記第 3 又は第 4 ビット列のビット数より少ないビット数の第 5 ビット列を前記第 1 鍵又は前記第 1 鍵の一部として出力する第 2 ステップとからなることを特徴とするコンテンツ情報復号化方法である。

【0016】

また、第 6 の発明は、暗号化した第 1 鍵のもとになる情報を第 2 鍵で復号化すると共に、復号化後の第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、

前記第 1 鍵を生成するにあたって、多数のビットからなる第 1 ビット列を有する前記鍵のもとになる情報を、前記第 1 ビット列よりビット数の少ない複数のビットからなる第 2 ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第 2 ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第 2 ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第 1 ビット列よりビット数が少ないビット数の第 3 ビット列を出力する S - B o x と、前記 S - B o x から出力した前記第 3 ビット列を入力するか、又は前記第 3 ビット列をこれよりビット数が少ないビット列に分割した第 4 ビット列を入力し、前記第 3 又は第 4 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 3 又は第 4 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 3 又は第 4 ビット列のビット数より少ないビット数の第 5 ビット列を前記第 1 鍵又は前記第 1 鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報復号化装置である。

【0017】

また、第 7 の発明は、上記した第 3 の発明のコンテンツ情報暗号化方法、もしくは、第 4 の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第 1 鍵のもとになる情報とを記録媒体に記録したことを

特徴とするコンテンツ情報記録媒体である。

【0018】

また、第8の発明は、上記した第3の発明のコンテンツ情報暗号化方法、もしくは、第4の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第1鍵のもとになる情報とを伝送路を介して送信することを特徴とするコンテンツ情報伝送方法である。

【0019】

【発明の実施の形態】

以下に本発明に係る鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法の一実施例を図1乃至図3を参照して詳細に説明する。

【0020】

図1は本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【0021】

まず、図1を用いて本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法について説明する。

【0022】

図1において、記録側または送信側とは、著作権を有するコンテンツ情報（以下、デジタル情報と記す）を暗号して、暗号化したデジタル情報を磁気テープ、磁気ディスク、光ディスク、カード等の記録媒体（コンテンツ情報記録媒体）に記録する側を示し、または、暗号化したデジタル情報をネットワーク（インターネット、電話回線）、電波、光無線などの伝送路に送信する側を示しており、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置と対応する側である。

【0023】

一方、再生側または受信側とは、記録側で暗号化したコンテンツ情報を記録した記録媒体を再生する側を示し、または、送信側で暗号化したコンテンツ情報を伝送路を介して受信する側を示しており、コンテンツ情報復号化方法、コンテンツ情報復号化装置と対応する側である。

【 0 0 2 4 】

まず、記録側または送信側において、デジタル化された映像信号や音声情報など著作権を有するデジタル情報 0 4 は、暗号化鍵である第 1 鍵 K 1 を用いて第 1 暗号化装置 0 5 によって暗号化される。この際、第 1 鍵 K 1 は、第 1 鍵のもとになる情報 0 1 から後述する一方向性関数 0 3 を用いて生成される。

【 0 0 2 5 】

また、第 1 鍵のもとになる情報 0 1 は、システム固有の第 2 鍵（以下、システム鍵と記す）K 2 を用いて暗号化される。このシステム鍵 K 2 は、システム固有の ID などを用いて生成した暗号化鍵である。

【 0 0 2 6 】

そして、第 1 鍵 K 1 を用いて第 1 暗号化装置 0 5 によって暗号化したデジタル情報 0 7 と、システム鍵 K 2 を用いて第 2 暗号化装置 0 2 によって暗号化した第 1 鍵のもとになる情報 0 6 とが、記録側で磁気テープ、磁気ディスク、光ディスク、カード等の記録媒体に記録されて再生側に提供されるか、または、ネットワーク（インターネット、電話回線）、電波、光無線などの伝送路を介して送信されて受信側で受信される。

【 0 0 2 7 】

次に、再生側または受信側において、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化された第 1 鍵のもとになる情報 0 6 は、第 2 復号化装置 0 8 でシステム固有の第 2 鍵（システム鍵）K 2 を用いて第 1 鍵のもとになる情報 0 9 に復号化される。ここで用いられるシステム鍵 K 2 も、システム固有の ID などを用いて生成した復号化鍵であり、且つ、記録側または送信側で暗号化時に用いたシステム鍵 K 2 と等価のものである。

【 0 0 2 8 】

また、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化さ

れたデジタル情報 0 7 は、復号化鍵である第 1 鍵 K 1 を用いて第 1 復号化装置 1 1 で元のデジタル情報（コンテンツ情報） 1 2 に復号化される。この際、第 1 鍵 K 1 は、第 2 復号化装置 0 8 から出力された復号化後の第 1 鍵のもとになる情報 0 9 から後述する一方向性関数 1 0 を用いて生成され、且つ、記録側または送信側で暗号化時に用いた第 1 鍵 K 1 と等価のものである。

【 0 0 2 9 】

上記した暗号化及び復号化において、システム鍵 K 2 は予め、記録側または送信側と、再生側または受信側で共通になるよう設定しておいても良く、更に、既知の公開鍵暗号方式や鍵配送方式を用いてもかまわない。

【 0 0 3 0 】

次に、本発明の要部をなす上記した第 1 鍵 K 1 を生成する鍵情報生成方法及び鍵情報生成装置について、図 2 乃至図 3 を用いて説明する。

【 0 0 3 1 】

図 2 は図 1 に示した第 1 鍵を生成する鍵情報生成方法を説明するための具体例を示した図、

図 3 は第 1 鍵を生成する鍵情報生成装置の具体例を示したブロック図である。

【 0 0 3 2 】

上記したように、第 1 鍵 K 1 は暗号化前のデジタル情報 0 4 への暗号化及び暗号化したデジタル情報 0 7 への復号化に用いられる鍵情報であり、この第 1 鍵 K 1 は先に説明した一方向性関数 0 3， 1 0 を適用しているものの、本発明に係る鍵情報生成方法及び鍵情報生成装置では、従来技術で説明した D E S 暗号化方法における S - B o x を適用した第 1 ステップと、本発明で新たに開発した第 2 ステップとを組み合わせ第 1 鍵 K 1 を生成することを特徴とするものである。

【 0 0 3 3 】

まず、図 2 に示した本発明に係る鍵情報生成方法は、一方向性関数を用いて第 1 鍵 K 1 を生成するにあたって、第 1 鍵のもとになる情報 0 1（又は 0 9）を入力して、ここで入力した多数のビットからなるビット列を基にして、第 1，第 2 ステップを経て、第 1 ステップで入力したビット列のビット数より極めて少ない

ビット数のビット列を生成して、これを第1鍵K1にすることを示している。

【0034】

即ち、図2及び図3に示した本発明に係る鍵情報生成方法及び鍵情報生成装置の具体例において、まず、第1ステップでは従来技術で説明したDES暗号化方法におけるS-Boxを適用している。

【0035】

上記した第1ステップにおいて、多数のビットからなる第1ビット列を有する第1鍵のもとになる情報01（又は09）を、この第1ビット列よりビット数が少ない複数のビットを有する第2ビット列に順次分割して、分割した各第2ビット列を鍵情報生成装置30に設けたS-Box31に分割した順に入力している。

【0036】

また、上記したS-Box31は内部に二次元のテーブルTを持ち、且つ、テーブルTは、従来例で説明したと同様に、指定した行列の各部位に対応して第2ビット列より少ないビット数からなる一つの要素値Hが予め設定されている。

【0037】

ここで、入力した各第2ビット列ごとに、第2ビット列の複数のビットを用いて所定の規則に従ってテーブルTの行と列とを指定している。この際、第2ビット列の複数のビットを用いてテーブルTの行と列とを指定するための所定の規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

【0038】

そして、分割した一つの第2ビット列によって指定された行列に対応した部位から一つの要素値Hを後述する第2ステップ側の論理演算部32側へ出力し、これを分割した各第2ビット列ごとに繰り返して複数の要素値Hで合成した第3ビット列を論理演算部32側への入力としている。

【0039】

これにより、第1ステップでは、多数のビットを有する第1ビット列からこれよりビット数が少ない第2ビット列に順次分割した後に、分割した各第2ビット

列を $S-B \times 31$ に順次入力して、 $S-B \times 31$ から出力する時には入力した第1ビット列よりビット数が少ないビット数の第3ビット列に変換されることになる。

【0040】

即ち、具体例における第1ステップにおいて、第1鍵のもとになる情報01（又は09）は、各ビットが“0”又は“1”のバイナリーデータで例えば200ビットからなる第1ビット列を形成しており、この第1ビット列を例えば8ビットを有する第2ビット列に順次分割して、25個の第2ビット列を $S-B \times 31$ に順次入力している。

【0041】

ここで、 $S-B \times 31$ に入力した1番目の第2ビット列が例えば $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8$ とすると、8ビットの $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8$ のうちで $a_1 a_2 a_3 a_4$ の4ビットでテーブルTの行を指定し、 $a_5 a_6 a_7 a_8$ の4ビットでテーブルTの列を指定している。

一方、テーブルT内では、第2ビット列により指定した行列に対応した部位の要素値Hを0から15までの整数、すなわち16進数で表せば、0からfの4ビットの値として予め設定されている。

そして、1番目の第2ビット列で指定した行列に対応した部位（ $a_1 a_2 a_3 a_4$ 行 $a_5 a_6 a_7 a_8$ 列成分）の4ビットからなる1番目の要素値Hとして $b_{11} b_{12} b_{13} b_{14}$ を $S-B \times 31$ から出力し、この後、2番目の第2ビット列で2番目の要素値Hとして $b_{15} b_{21} b_{22} b_{23}$ を出力し、更にこの後、上記した第1ステップを23回繰り返して、ここで得られた全部で25個の各要素値Hを合成することで、入力した第1ビット列よりビット数が少ない100ビットからなる第3ビット列が得られ、これを後述する第2ステップの論理演算部32側への入力ビット列としている。

【0042】

尚、上記した第1ステップでは、200ビットの第1ビット列を8ビットづつ分けて説明したが、入力した第1ビット列のビット数及び第1ビット列を分割した第2ビット列のビット数は適宜設定されるものである。また、第1ビット列を

分割した各第2ビット列を同一のテーブルTで上記と同様に処理するか、または、異なるテーブルで処理しても良い。更に、テーブルT内の各要素値Hは、入力ビット数より少ないビット数で0から15以外の数を出力値として設定しても良い。

【0043】

次に、本発明で新たに開発した第2ステップでは、第1ステップで得られた複数のビットを有する第3ビット列を鍵情報生成装置30に設けた論理演算部32にそのまま入力するか、又は、第3ビット列より少ないビット数からなる第4ビット列に順次分割して、分割した複数の第4ビット列のうちで一部の第4ビット列を論理演算部32に入力するか、もしくは、複数の第4ビット列を論理演算部32に順次入力している。

【0044】

上記した論理演算部32では、入力した第3又は第4ビット列の各ビットを、行列を有する第1マトリックスM1内に所定の配列規則に従って配置している。この際、第1マトリックスM1内に第3又は第4ビット列の各ビットを配置するための所定の配列規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

この後、第1マトリックスM1内で入力した第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに順に論理演算する。そして、論理演算して得られた各結果のビットを、第1マトリックスM1より行列を小さくした第2マトリックスM2内にブロック順に配置して、第2マトリックスM2内の各ビットから第3又は第4ビット列のビット数より少ないビット数の第5ビット列を生成して第1鍵K1又は第1鍵K1の一部として出力している。

【0045】

これにより、第2ステップでは、第1ステップで得られた第3ビット列又は第3ビット列よりビット数を少なくして分割した第4ビット列を論理演算部32に入力して、論理演算部32から出力する時には、第1、第2ステップの入力ビットよりビット数が少ない第5ビット列に変換されて、第1鍵K1又は第1鍵K1

の一部として出力されることになる。

【0046】

即ち、具体例における第2ステップでは、第1ステップで得られた100ビットを有する第3ビット列を例えば25ビットごとに分割し、分割して得られた第3ビット列を論理演算部32に入力している。

【0047】

尚、具体例における第2ステップで第1ステップで得られた第3ビット列を論理演算部32にそのまま入力する場合には、第3ビット列のビット数が第1ステップの入力ビット数よりも少なく、しかも、この第3ビット列をこれより少ないビット数に分割する必要がある場合であるが、この第3ビット列の複数のビットを第1マトリックスM1内に所定の配列規則に従って配置して以下の記載と同様に処理するものであるので、この場合の説明を省略する。

【0048】

ここで、第1ステップで得られた100ビットを有する第3ビット列から分割して1番目に入力した25ビットの第4ビット列を、最上位から順に $b_{11} b_{12} b_{13} b_{14} b_{15} b_{21} b_{22} b_{23} b_{24} b_{25} \dots b_{51} b_{52} b_{53} b_{54} b_{55}$ とし、各ビットの値は“0”又は“1”のバイナリデータとする。

【0049】

そして、入力した25ビットからなる第4ビット列のうちで例えば $b_{11} b_{12} b_{13} b_{14} b_{15}$ を第1マトリックスM1内の第1行目に列に沿って配置し、 $b_{21} b_{22} b_{23} b_{24} b_{25}$ を第2行目に列に沿って配置し、以下同様に順次繰り返して、 $b_{51} b_{52} b_{53} b_{54} b_{55}$ を第5行目に列に沿って配置することで、入力した各ビットを第1マトリックスM1内に5×5のビットマトリックスとして配置している。

【0050】

この後、第1マトリックスM1内で入力した第4ビット列のビット数より少ないビット数で例えば $b_{11} b_{12} b_{21} b_{22}$ を第1ブロックとして形成して、 b_{11} と b_{12} と b_{21} と b_{22} とで排他的論理和を取り、この排他的論理和の結果のビット c_{11} を第2マトリックスM2内の第1行、第1列目に配置する。次に、第1ブロックに対して列を1列ずらした $b_{12} b_{13} b_{22} b_{23}$ を第2ブロックとして形成して、上

記と同様に論理演算した結果のビット c_{12} を第 2 マトリックス M_2 内の第 1 行第 2 列目に配置する。上記のように、列方向に沿って 4 ブロックの論理演算処理が終わったら、1 行ずらして再び上記処理を順次繰り返し、合計で 16 ブロックの論理演算処理が全て終了すると、第 2 マトリックス M_2 内に 4×4 のビットマトリックスが形成される。この後、第 2 マトリックス M_2 内の 4×4 のビットマトリックスから第 5 ビット列として 16 ビットからなる $c_{11} c_{12} c_{13} c_{14} c_{21} c_{22} c_{23} c_{24} c_{31} c_{32} c_{33} c_{34} c_{41} c_{42} c_{43} c_{44}$ を生成して、この第 5 ビット列を論理演算部 32 から第 1 鍵 K_1 として出力するか、又は、第 1 鍵 K_1 の一部として出力している。

【 0 0 5 1 】

この際、論理演算部 32 から第 1 鍵 K_1 の一部として出力する場合には、1 番目の第 4 ビット列以外の残りのいくつかの第 4 ビット列を上記と同様に処理して、これらを合成して最終的に第 1 鍵 K_1 として論理演算部 32 から出力するものであり、例えば 1 番目～4 番目の第 4 ビット列を用いた場合には第 1 鍵 K_1 が 64 ビットとなり、この場合でも第 1 鍵 K_1 は第 1、第 2 ステップで入力したビット数よりも少ないビット数に削減されている。

【 0 0 5 2 】

尚、具体例における第 2 ステップでは、論理演算部 32 に入力した第 4 ビット列のビット数を 25 ビットとしたがこれに限ることなく、第 1 ステップの入力ビット数より少ない適宜なビット数でも良い。また、第 1 マトリックス M_1 内で入力した 25 ビットを第 4 ビット列の最上位から最下位に向かって順に配置して説明したが、これに限ることなく、所定の配列規則に従って配置しても良い。また、第 1 マトリックス M_1 内に形成した各ブロックごとの論理演算も排他的論理和 (EX-OR) に代えて論理和 (OR) 又は論理積 (AND) で行っても良い。

【 0 0 5 3 】

そして、論理演算部 32 から出力され、一方向性関数により生成された第 1 鍵 K_1 は、第 1 暗号化装置 05 でデジタル情報 04 の暗号化に用いられ、また、第 1 復号化装置 11 で暗号化したデジタル情報 07 の復号化に用いられている。
尚、実施例では暗号化を 2 段としたが、第 $n-1$ 鍵 (但し、 n は 3 以上の整

数)のもとになる情報を第n暗号化装置で暗号化する場合、第n鍵をのもとになる情報から第n鍵を生成するのに、上記の一方向性関数を用いたシステムを構築することも可能である。

【0054】

【発明の効果】

以上詳述した本発明に係る鍵情報生成方法、コンテンツ情報暗号化方法、コンテンツ情報復号化方法によると、とくに、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報(第1鍵)を、鍵(第1鍵)のもとになる情報から一方向性関数を用いて生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力する第1ステップと、前記第1ステップで出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記鍵情報(第1鍵)又は前記鍵情報(第1鍵)の一部として出力する第2ステップとで行っているので、本発明により容易にシステムに応じた量のビット数を少ないステップ数でかつセキュリティを保持したまま減少させることが可能な一方向性関数を実現することができる。そしてこの一方向性関数は入力ビットの“0”と“1”の割合を出力に直接反映させないため、暗号化鍵及び復号化鍵に利用するのに好適で、かつ

鍵（第1鍵）のもとになる情報は必要な鍵のサイズに関係なく設定することが可能となる。また、一方向性関数内のビット演算の方法や置換によって、より鍵生成のメカニズムのセキュリティを高めることができる。

【0055】

また、本発明に係る鍵情報生成装置、コンテンツ情報暗号化装置、コンテンツ情報復号化装置によると、とくに、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第1鍵）を、鍵（第1鍵）のもとになる情報から一方向性関数を用いて生成するにあたって、多数のビットからなる第1ビット列を有する前記鍵のもとになる情報を、前記第1ビット列よりビット数の少ない複数のビットからなる第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第2ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第2ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第1ビット列よりビット数が少ないビット数の第3ビット列を出力するS-B o xと、前記S-B o xから出力した前記第3ビット列を入力するか、又は前記第3ビット列をこれよりビット数が少ないビット列に分割した第4ビット列を入力し、前記第3又は第4ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第3又は第4ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第3又は第4ビット列のビット数より少ないビット数の第5ビット列を前記鍵情報（第1鍵）又は前記鍵情報（第1鍵）の一部として出力する論理演算部とを備えているので、上記した各方法で述べた効果と同様の効果を得ることができる。

【0056】

また、本発明に係るコンテンツ情報記録媒体、コンテンツ情報伝送方法によれば、上記した第1鍵を用いて暗号化したコンテンツ情報と、暗号化した第1鍵のもとになる情報とを記録媒体に記録するか、または、伝送路を介して送信してい

るので、コンテンツ情報のセキュリティを高めることができる。

【図面の簡単な説明】

【図 1】

本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【図 2】

図 1 に示した第 1 鍵を生成する鍵情報生成方法を説明するための具体例を示した図である。

【図 3】

第 1 鍵の生成する鍵情報生成装置の具体例を示したブロック図である。

【図 4】

一般的な DES (Data Encryption Standard) 暗号化方法に用いられている S-Box を示したブロック図である。

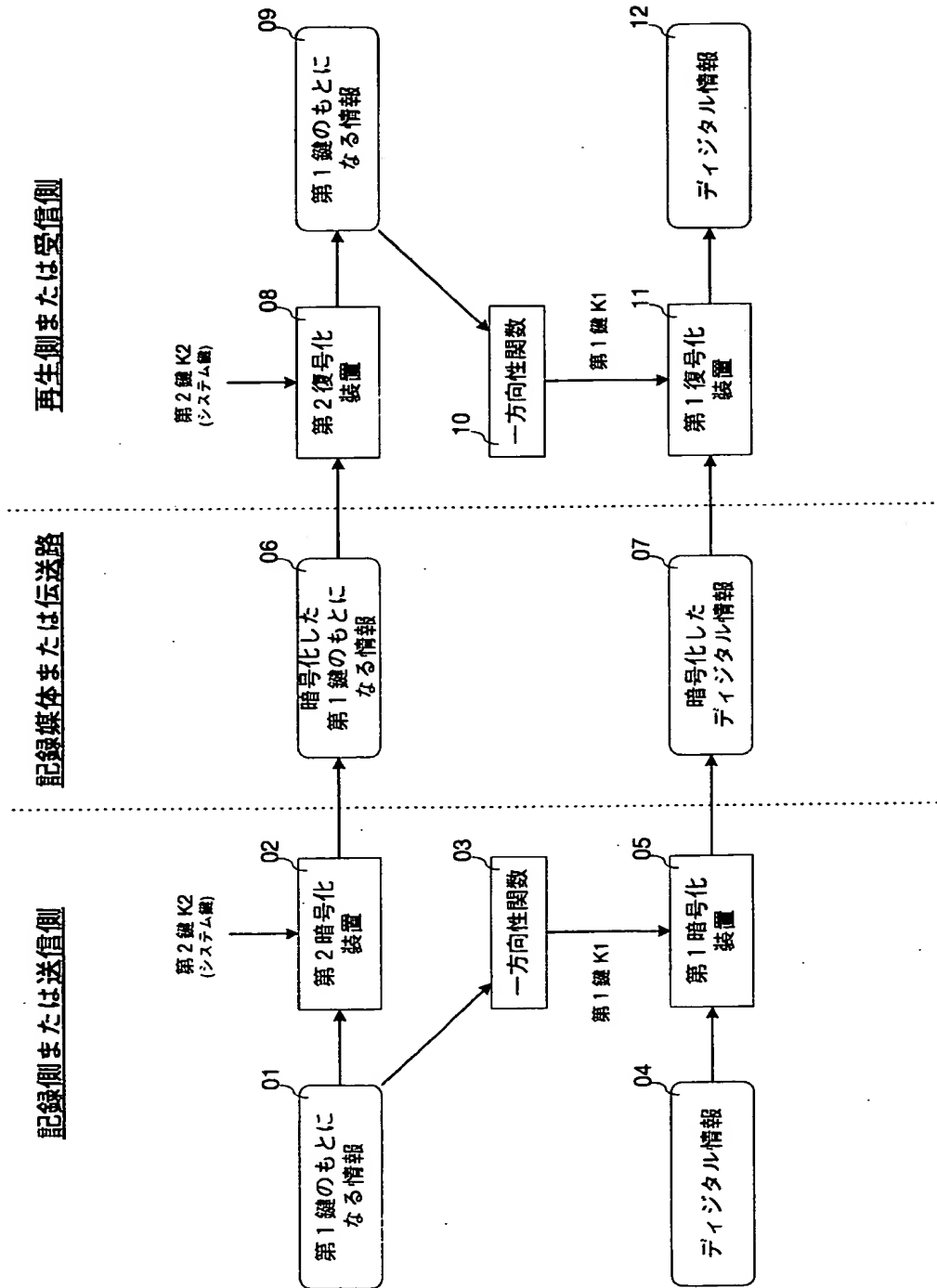
【符号の説明】

0 1 … 第 1 鍵のもとになる情報、 0 2 … 第 2 暗号化装置、
 0 3 … 一方向性関数、 0 4 … コンテンツ情報（デジタル情報）、
 0 5 … 第 1 暗号化装置、 0 6 … 暗号化した第 1 鍵のもとになる情報、
 0 7 … 暗号化したデジタル情報、 0 8 … 第 2 復号化装置、
 0 9 … 第 1 鍵のもとになる情報、 1 0 … 一方向性関数、
 1 1 … 第 1 復号化装置、 1 2 … コンテンツ情報（デジタル情報）、
 3 0 … 鍵情報生成装置、 3 1 … S-Box、 3 2 … 論理演算部、
 K 1 … 第 1 鍵、 K 2 … 第 2 鍵（システム鍵）、
 M 1 … 第 1 マトリックス、 M 2 … 第 2 マトリックス、
 T … テーブル。

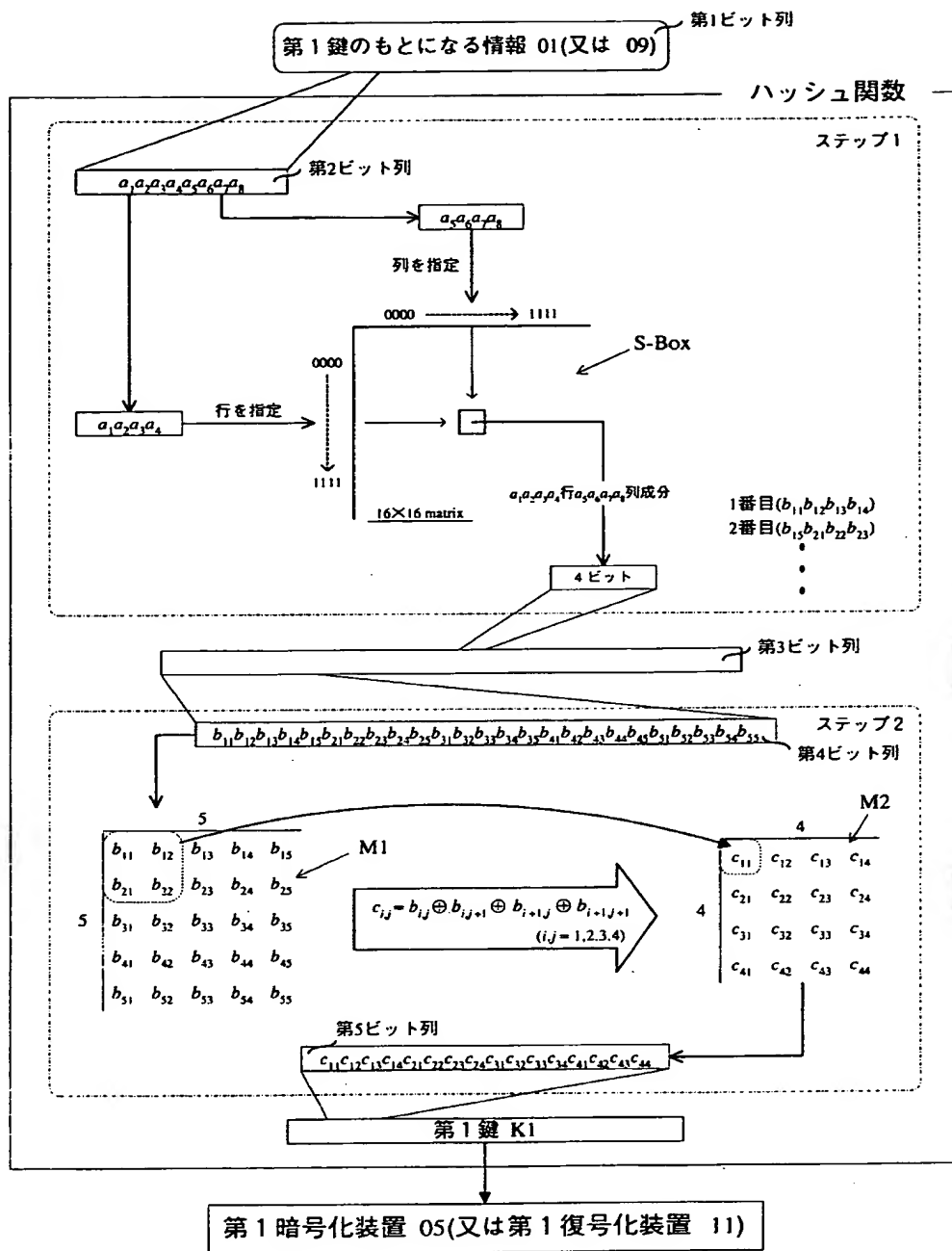
【書類名】

図面

【図 1】

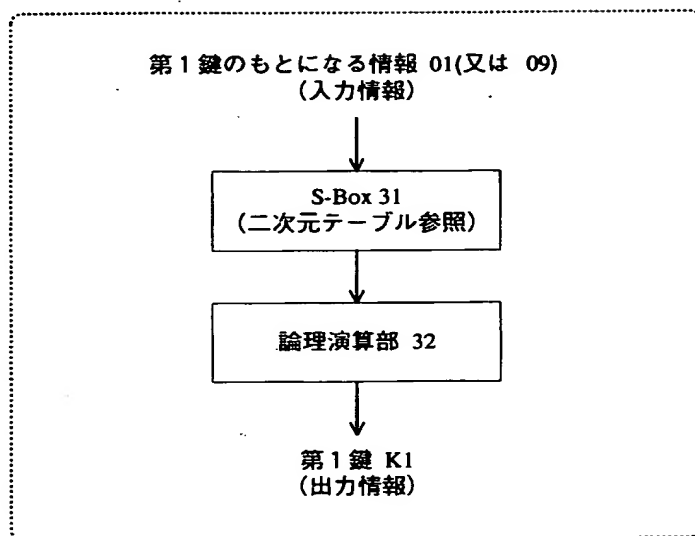


【図 2】

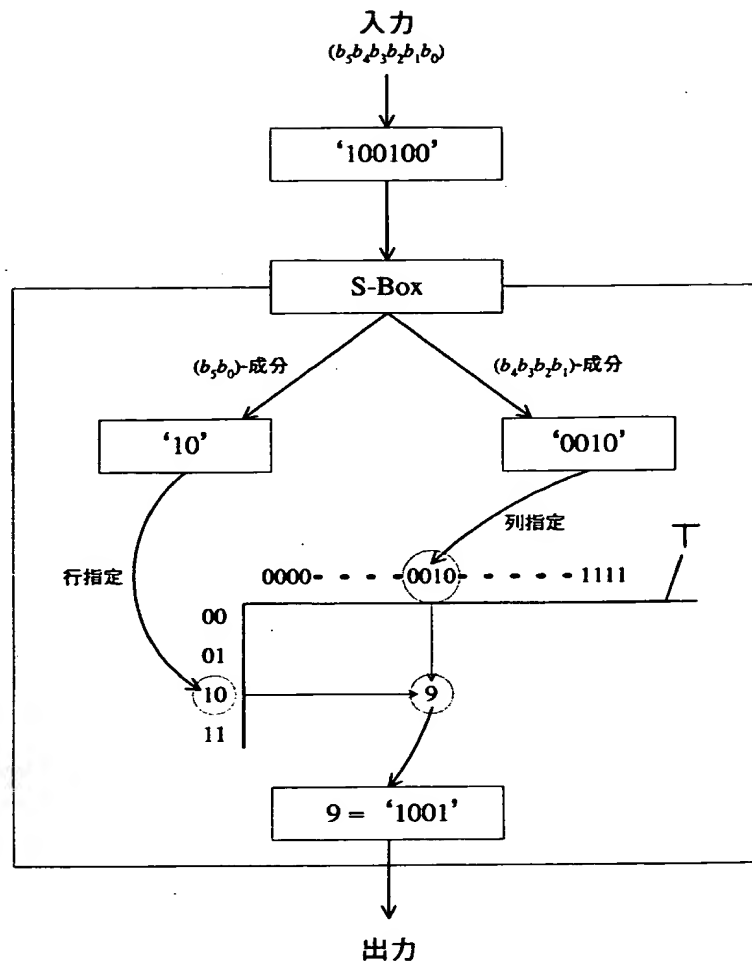


【図 3】

鍵情報生成装置 30



【図 4】



【書類名】 要約書

【要約】

【課題】 鍵情報を一方向性関数を用いて生成する。

【解決手段】 第1ビット列よりビット数の少ない第2ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて各要素値を予め設定しておき、各第2ビット列の複数のビットを用いてテーブルの行と列とを指定すると共に、各第2ビット列で指定した行列の部位と対応して得た各要素値を合成した第3ビット列を出力する第1ステップと、第1ステップで出力した第3ビット列を入力するか、又は第3ビット列をこれよりビット数が少ない第4ビット列に分割して入力し、第3又は第4ビット列の各ビットをマトリックス内に配置し、且つ、マトリックス内で第3又は第4ビット列のビット数より少ない複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算した各結果のビットで第3又は第4ビット列のビット数より少ない第5ビット列を出力する第2ステップとからなる。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日 1990年 8月 8日

[変更理由] 新規登録

住 所 神奈川県横浜市神奈川区守屋町3丁目12番地

氏 名 日本ビクター株式会社